(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 320 008 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.06.2003 Bulletin 2003/25

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **02258089.8**

(22) Date of filing: **25.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **05.12.2001 US 17438**

(71) Applicant: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

(72) Inventors:
- **Iwamoto, Neil Y., c/o Canon Development**
  Irvine, California 92612 (US)
- **Seikh, Attaullah, c/o Canon Development**
  Irvine, California 92612 (US)
- **Paek, Jeanette Y., c/o Canon Development**
  Irvine, California 92612 (US)
- **Martinez, Martin, c/o Canon Development**
  Irvine, California 92612 (US)
- **Slick, Royce E., c/o Canon Development**
  Irvine, California 92612 (US)
- **Chern, Wei-Jhy, c/o Canon Development**
  Irvine, California 92612 (US)
- **Khosrova, Eliza, c/o Canon Development**
  Irvine, California 92612 (US)
- **Yang, Joseph, c/o Canon Development**
  Irvine, California 92612 (US)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
2-5 Warwick Court,
High Holborn
London WC1R 5DH (GB)

(54) Centralized authentication for authorising access to network peripheral devices

(57) Access control to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user, based on centralized access management information. Access control comprises receiving authenticated information for the walk-up user from the networked peripheral device at a centralized location, determining at the networked peripheral device a level of access to the networked peripheral device by the walk-up user based on received access management information for the walk-up user, and allowing the walk-up user to access the determined user-available features of the networked peripheral device based on the determined level of access.

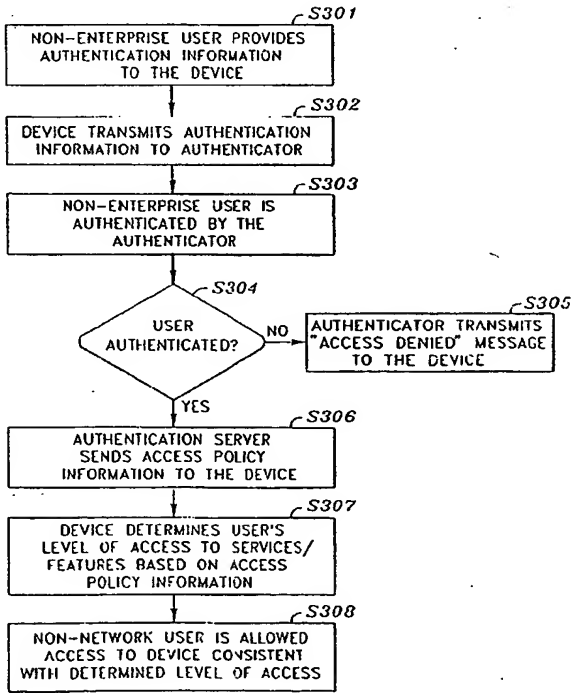

FIG. 4

EP 1 320 008 A2

Description

[0001] The invention relates to a centralized authentication mechanism. More particularly, the invention relates to use of a centralized authentication mechanism for providing user privileges information to a networked peripheral device.

[0002] Networked peripheral devices are typically multifunction devices that handle functions such as printing, scanning, copying or faxing and are often relied upon in performing enterprise level tasks. Controlling usage of a networked peripheral device means that a walk-up user of the device, i.e., one that gains access to the device locally at the device, or a remote user of the device, i.e., a non walk-up user, is allowed access to only those services and/or features available on the device that are authorized. For example, a user may have access to copying but not a printing service of a networked peripheral device that offers faxing, printing, copying and scanning services. Likewise, a user may only be allowed access to a black-and-white, but not a color printing feature of the printing service offered by the device.

[0003] Controlling usage of services and/or features offered by a networked peripheral device is often necessary for economic as well as other reasons. For example, color ink cartridges containing ink for color printing typically cost significantly more than black ink cartridges that are used for black and white printing. It may therefore be desirable to limit access to color printing features of a printer in order to save costs.

[0004] One conventional approach to controlling access to a networked peripheral device by a non-enterprise user is to program each device separately as to the access privileges of the user. This approach requires presence of an input mechanism such as a keyboard or a magnetic card reader on the device through which the user logs into the device. Following login by the user, the device examines the user's access privileges, which are maintained by the device, and allows the user access to the device based on the programmed information concerning the user's access privileges. Adoption of this approach is cumbersome since it requires separate programming of each networked peripheral device and reprogramming of each device in response to changes in access policy.

[0005] Another conventional approach to controlling access to a networked peripheral device by a non-enterprise user is to program user access privileges on a keycard that is carried by the user. Upon swiping the keycard on a card reader installed on the device, the user access policy is transmitted from the card to the device. The user is then allowed to use the device in accordance with the limitations contained in the user access policy. This approach also suffers from the drawback suffered by the previous alternative in that each individual card needs to be programmed in order to encode user access policy and reprogrammed each time the policy is revised as to that user. It would therefore be beneficial to be able to control and customize access to services and/or features of a networked peripheral device by a non-enterprise user using a centralized mechanism, which provides both enterprise user authentication and non-enterprise user authentication and access privilege information to manage device/resource usage, at the enterprise level.

[0006] The present invention addresses the above inadequacies by providing a centralized level of access management to networked peripheral devices for both walk-up and remote users in order to prevent unauthorized use by a non-enterprise user of services and/or features that are available on a device based on authentication of the user at the device.

[0007] In one aspect, the invention concerns creating a context-sensitive user interface for a networked peripheral device. The user supplies authentication information to a device via any input means including, but not limited to, a keypad, a smart card, or any other input method that is supported by the device. The device communicates the authentication information provided by the user to an authentication server, which provides authentication services for both walk-up and remote for users of the device, and where networked peripheral device access policy information for users is stored. Access policy information is in turn transmitted to the device, which determines the level of access of a user based on the received access policy information.

[0008] The access policy information may concern access to a service offered by the networked peripheral device itself or to certain features of services available on the device. Upon authentication of the user by the authentication server, the information (e.g., privilege information or other access policy information) about the user's level of access to the device is passed back to the device. The device determines the user's access to services/ features of the device based on the privilege information supplied by the authentication server. The device can create a customized user interface such as a customized service menu for the user that incorporates access policy information for the user. The customized service menu is then displayed on the device, allowing the user access to the determined features.

[0009] Providing a centralized location for access management information for use by a networked peripheral device in order to prevent unauthorized use of device services/features based on authentication of the user addresses the current problems associated with controlling access to a networked peripheral device by a walk-up user and eliminates the need for individual programming of each device or keycard in response to changes in access policy.

[0010] This brief summary has been provided so that the nature of the invention may be understood quickly. A more complete understanding of the invention can be obtained by reference to the following detailed description of preferred embodiments which are described by

BNSDOCID: <EP_____1320008A2_I_>

way of example only with reference to the attached drawings in which:

Figure 1 is a view showing the outward appearance of a representative hardware embodying the present invention.

Figure 2 is a detailed block diagram showing the internal architecture of the computer shown in Figure 1 in accordance with an embodiment of the present invention.

Figure 3 is a block diagram showing an overview of components for use in managing and/or controlling access to network peripheral devices according to an embodiment of the present invention.

Figure 4 illustrates a flow diagram of process steps to manage and/or control access to a networked peripheral device by a walk-up user according to an embodiment of the present invention.

Figure 5 is a screen shot of the display screen showing a UI at a stage prior to walk-up user login to the device.

Figure 6 is a screen shot of the display screen showing a UI through which a walk-up user would log into the device.

Figure 7 is a screen shot of the display screen showing a customized service menu corresponding to services/features available to a walk-up user.

Figure 8 is a screen shot of the display screen showing another customized service menu corresponding to services/features available to a walk-up user.

Figure 9 is a screen shot of the display screen showing a UI through which walk-up user would log out of the device.

Figure 10 illustrates a flow diagram of process steps of a networked peripheral device to manage and/or control access to the device by a walk-up user according to an embodiment of the present invention.

Figure 11 illustrates a flow diagram of process steps to manage and/or control access to a networked peripheral device by a remote user according to an embodiment of the present invention.

Figure 12 illustrates a flow diagram of process steps of a networked peripheral device to manage and/or control access to the device by a remote user according to an embodiment of the present invention.

Figure 13 illustrates a flow diagram of process steps of a server to manage and/or control access to the device by a remote user or a walk-up user according to an embodiment of the present invention.

[0011] Figure 1 is a view showing the outward appearance of a representative hardware embodying the present invention. Computing equipment 1 includes host processor 9 comprising a personal computer (hereinafter "PC") preferably having windowing operating system such as Microsoft Windows 2000®, Windows ME®, etc. operating system. Provided with the computing equipment 1 are color monitor 2 including display screen 10, keyboard 4 for entering text data and user commands, and pointing device 16. Pointing device 16 preferably comprises a mouse, for pointing, selecting and manipulating objects displayed on display screen 10.

[0012] Computing equipment 1 includes a computer-readable memory medium such as a fixed disk 17 and/or floppy disk drive 20 and/or CD-ROM drive 19. Such computer readable memory media allow computing equipment 1 to access information such as user-related data, computer executable process steps, application programs, and the like, stored on removable and non-removable memory media. In addition, computing equipment 1 is connected to server 8 through an enterprise network 7 and can acquire information and application programs from the server 8 through network 7. Enterprise network is preferably an Intranet but can also be a Local Area Network (LAN), a Wide Area Network (WAN) or the Internet, for example. The computing equipment 1 is connected to networked peripheral device 6 through the network 7. Device 6 includes one or more buttons 11, which may be programmable. As is discussed in more detail below, buttons 11 may be enabled or disabled by device 6 depending on the received access policy.

[0013] Like computing equipment, server 8 is a computer preferably having a windowing operating system. The server 8 has a storage device 41, which is preferably a large fixed disk for storing files. While device 41 is shown to be external to server 8, it need not be. Other devices on the network 7 can therefore use the server 8 as a file server and for storing applications such as an authenticator configured to authenticate a user and for storing user and device configuration information on a directory service, which is described in more detail with reference to Figure 3, and which directory service contains such information as user account information and access policy information. The directory service is preferably a Microsoft Active Directory, which is a component of the Windows 2000® that provides directory services to a Windows environment. In addition to providing for central management and sharing of information on network resources and users, Microsoft Active Directory® acts as the central authority for network security that will be discussed below with reference to Figure 4.

[0014] The interface between the directory service,

BNSDOCID: <EP_____1320008A2_I_>

which contains authentication and access policy information, and other components is provided by the authenticator, a component of server 8, which is responsible for authenticating users and providing access management information stored on the directory service. The authenticator is preferably located on server 8 with the directory service, but can also be implemented on a remote system, or server.

[0015] Figure 2 is a detailed block diagram showing the internal architecture of computing equipment 1. As shown in Figure 2, computing equipment 1 includes central processing unit ("CPU") 20 that interfaces with computer bus 25. Also interfacing with computer bus 25 are fixed disk 3. network interface 21 for accessing network 7, random access memory ("RAM") 30 for use as main memory. read only memory ("ROM") 29, floppy disk interface 28. CD-ROM interface 24, display interface 26 to monitor 10 keyboard interface 22 to keyboard 4, mouse interface 27 to pointing device 16, and peripheral device interface 23 to a stand alone, non-networked device 6.

[0016] Main memory 30 interfaces with computer bus 25 so as to provide RAM storage to CPU 20 during execution of software programs such as the operating system, application programs, and device drivers. More specifically, CPU 20 loads computer-executable process steps from disk 3 or other memory media into a region of main memory 30, and thereafter executes the stored process steps from main memory 30 in order to execute software programs. Data can be stored in main memory 29, where the data can be accessed by CPU 20 during execution. As also shown in Figure 2, fixed disk 3 contains a windowing operating system 51, application programs 52 such as application word processing, spreadsheet, database, imaging, graphics, etc. applications, and device drivers 53 such as networked peripheral device driver 54.

[0017] Figure 3 is a block diagram showing an overview of components for use in managing and/or controlling access to network peripheral devices according to an embodiment of the present invention. Briefly, server 8 includes a host processor (not shown) that has a windowing operating system. The server 8 uses storage device 41, which is a preferably a large fixed disk for storing numerous files, to store directory service 47. Directory service 47 contains user access policy information and other information such as user authorization information. Access policy information refers to access control information (e.g., rules) that has been defined at an enterprise level concerning user access to services/features available on the networked peripheral device 6. For example, a user may have access to a copying but not a printing service of a multifunction networked peripheral device 6 that offers faxing, printing, copying and scanning services. Likewise, a user may only be allowed access to a black-and-white printing feature, but not a color printing feature, of a printing service available on the device 6.

[0018] The device 6 includes an access controller 66, which allows the user to access the device consistent with the determined level of access. Access controller is preferably an embedded computer system with an internal architecture similar to that shown in Figure 2 including some or all of the interfaces shown. The access controller 66 controls user access to services/features available on the device 6 based on the access policy information provided to it by server 8. Access controller 66 may enforce the access policy associated with a user through creation of a user interface that is customized according to the user's level of access. Alternatively, access controller 66 may disable/enable buttons (e.g., button 11) on or displayed by, device 6. Of course, a combination of a user interface and buttons disabling/enablings may also be used. Device 6 further comprises the components needed to perform the services/features of the device 6. In a case of a multifunction device, for example, device 6 further comprising scanning, printing, faxing and copying components.

[0019] According to Figure 3, the server 8 is connected to the computing equipment 1 and to networked peripheral device 6 through an enterprise network 7. The networked peripheral device 6 is preferably a multifunction device that offers faxing, copying, printing and scanning services but may be any type of networked peripheral device. Each of services offered by networked peripheral devices may include associated features. For example, printing may be available in color and black-and-white; scanning may be available in color, black-and-white and be available at various resolution levels. The following is an example of a structure of an enterprise access policy for use with a multi-functional networked peripheral device, which includes access/privilege information at both the service and feature levels.

Services	Features	Policy
Print	B/W	Y/N
	Color	Y/N
	Daily Quota (Pages)	0-2000
Scan	B/W	Y/N
	Color	Y/N
	Resolution	L, H/L, H
	Daily Quota (Pages)	0-100
Fax	Local	Y/N
	Long Distance	Y/N
	Resolution	H, H/L, L
	Daily Quota (Pages)	0-200
Copy	B/W	Y/N
	Color	Y/N
	Resolution	H, H/L, L
	Daily Quota	0-1500

BNSDOCID: <EP_____1320008A2_I_>

(continued)

Services	Features	Policy
	(Pages)	

[0020] In the above example, the print service includes black-and-white (i.e., B/W), color and daily quota features. The information under the policy column identifies whether or not the feature is available and/or a number from zero to two thousand that represents a daily quota (e.g., a number of pages) the number of pages the user is allowed. For example, a user may be limited to printing 200 pages in a single day.

[0021] In addition to features that are similar to those of the print service, the scan service is available at high (H), medium (H/L), and low (L) resolutions as indicated under the policy column (i.e., H, H/L, L). The daily quota feature for the scan service is between zero and one hundred pages. The Fax service includes local, long distance, and daily quota features. The information under the policy column identifies whether or not the feature is available and/or a number from zero to two hundred that represents the number of pages the user can fax. In addition to the features that are similar to those of the print service, the copy service is available at various H, H/L and L resolutions that are indicated under the policy column. The information under the policy column identifies whether or not the feature is available and/or a number from zero to two hundred that represents the number of pages the user can copy.

[0022] After the authenticator 48 has tested the user authentication information against the access policy information and transmitted the result back to the device 6, the access controller 66 determines the user's level of access to services/features available on the device 6 based on the access policy information received from the authenticator 48. The access controller 66 preferably enforces the enterprise access policy for the user by creating a customized user experience (e.g., customized UI, customized service menu) for the user. The customized service menu is then displayed on the device 6. Input/Output (I/O) unit 76 on the networked peripheral device 6 provides the customized service menu. I/O unit 76 may be an external unit that is attached to the device 6 but may also be built into the device 6, and may provide a display unit as well as input mechanism (e.g., keyboard and/or media reader).

[0023] The customized service menu allows the user to use the determined services and/or features available on the networked peripheral device 6 in accordance with enterprise access policy information for the user. The customized service menu is preferably displayed on a touch-screen that allows the user to activate the keys by touching virtual keys that are displayed on the screen on which the menu is displayed. In such a case, the user may gain access to the device 6 by activating the virtual keys that are displayed on the I/O unit 76 corresponding to available services/features on the device 6. However, keys can also be activated through other means such as use of a pointing device 16, where I/O unit 76 comprises computing equipment 1.

[0024] Generally, the I/O unit that is used at the device 6 can be non-integrated where the input and output functions are performed by separate units. For example, I/O unit 76 may comprise a separate keypad. I/O unit can also be integrated where the same unit performs both input and output functions. For example, I/O unit may be a touch screen that displays output including virtual keys that are activated in response to the user's touch.

[0025] A user of the networked peripheral device 6 can be a walk-up user or a remote user. A walk-up user is defined as one who gains access to the device 6 locally at the device. A remote user is a non-walk-up user. In the case of the walk-up user, as discussed in more detail with respect to Figure 4, the authentication information received by device 6 is transmitted from the device 6 to the authenticator 48 and device 6 receives access information policy from the authenticator 48. In the case of the remote user who may have already logged on to the network, device driver 54 requests access policy information that corresponds to the user and device 6 and provides authenticator 48 with user login and device information.

[0026] The authenticator 48 transmits access policy information to device driver 54. Authenticator 48 notifies device 6 of access policy associated with the authenticated user preferably along with the job, which was submitted by the user via device driver 54. If authenticator 48 is unable to authenticate a user based on the authentication information sent by device 6, it may send an "authentication failed" message or a "no services/features available," message, or both. Where the user is authenticated, the authenticator 48 forwards the access policy information along with the job request to the device 6. The device 6 then processes the job request to the extent it conforms to the access policy information.

[0027] Figure 4 illustrates a flow diagram of process steps to manage and/or control access to a networked peripheral device by a walk-up user according to an embodiment of the present invention. Before allowing the user to access the device 6, the request must be vouched for by a trusted application such as the authenticator 48, which is stored on the server 8. All authentication information is kept in a directory service 47 that exists on the server 8. A user initiates a job by providing authentication information to the networked peripheral device 6. The user can use any of the services that are available on the networked peripheral device 6, for which the user is authorized, and any feature corresponding to any of those services such as black-and-white or color features of a printing service, for which the user is authorized.

[0028] Since a walk-up user accesses the device directly, in step S301 a walk-up user provides authentica-

BNSDOCID: <EP_____1320008A2_I_>

tion information to the device 6. Preferably, a single, universal sign-on functionality is in effect according to which the authentication information is the user's username and password. In any case, the same authentication information may be used to authenticate a user for other purposes (e.g., access to server 8, or files stored thereon). Advantageously, a universal sign-on avoids entry of separate, unique user names/passwords for login at the device 6 and for any other purposes for which authentication is a prerequisite.

[0029] Step S302 causes the device 6 to communicate the authentication information provided by the user to the authenticator 48, which in turn determines if the user is an authorized user. The authenticator 48 accomplished this in step S303 by comparing or testing the authentication information provided by the user to access policy information stored in directory service 47. The enterprise access policy for the user may also be stored on the directory service 47 on the server 8.

[0030] Step S304 determines whether the user has been successful or unsuccessful in obtaining authentication from the authenticator 48. If the user is unsuccessful in obtaining authentication for the job request, the authenticator 48 preferably communicates this failure through an "access denied" message that is transmitted to the device 6 per step S305. If the user is successful in obtaining authentication, then in step S306 the authenticator 48 sends access policy information for the user back to the device 6.

[0031] The communication between the device 6 and the server 8 is conducted through a secure communication that minimizes chances of unauthorized access to the device by hackers. The preferred security mechanism implements an encryption mechanism for communications between the server 8 and the device 6. The encryption is preferably performed such that access information is stored at the directory service 47 in an encrypted form utilizing a cryptographic signing operation. The encrypted access policy information is then retrieved and sent by the authenticator 48 in an encrypted form to device 6, which decrypts the information upon receipt. In addition to encrypting access policy information, device 6 may encrypt authentication information before sending it to server 8.

[0032] Although the encryption is preferably performed such that the information stored at the directory service 47 is encrypted, it can alternatively be stored in non-encrypted form at the directory service 47. Accordingly, access policy information is stored in a non-encrypted form at the directory service 47 and is encrypted at the authenticator 48. Similarly, although the preferred security mechanism is an encryption mechanism, other feasible security mechanisms include transmission with secure socket layer ("SSL") capabilities, use of propriety protocols for communications between the server 8 and the device 6, and use of propriety mechanisms in connection with standard protocols.

[0033] Once the device 6 obtains the user access policy information from the authentication server 8, the access controller 66 proceeds in step S307 to determine user access to services and/or features offered by the device 6 based on the access policy information received from the authenticator 48. The following is an example of user access policy information for a multi-functional networked peripheral device:

Services	Features	Policy
Print	B/W	Y
	Color	Y
	Daily Quota	150
Scan	B/W	Y
	Color	N
	Resolution	L
	Daily Quota	50
Fax	Local	Y
	Long Distance	N
	Resolution	H/L, L
	Daily Quota	25
Copy	B/W	Y
	Color	N
	Resolution	H, H/L, L
	Daily Quota	500

[0034] In the above example, user is allowed to use both black-and-white and color features of the print service up to a daily maximum of 150 pages. The user can use the scan service for scanning up to 50 pages of black-and-white pages per day at low resolution, fax up to 25 pages a day as long as the faxes are not transmitted over long distance telephone line, and are transmitted at medium or low resolution, and can use the copying service to make up to 500 black-and-white copies a day at all resolutions.

[0035] In step S308 the user is allowed access to services/features of the device 6 consistent with the determined level of access. This may be implemented by the access controller 66 through creation of a user interface, which includes selections based on the access policy information obtained for the particular user. Accordingly, the device 6 creates a customized user interface such as a customized service menu for the user that incorporates the access policy for the user. The customized service menu is then displayed on the device 6 with services/features appearing as virtual keys on the I/O unit 76.

[0036] Figures 5-9 are views of the display screen 10 showing changes in a UI at various stages of a walk-up user's interaction with the device 6.

[0037] Figure 5 is a screen shot of the display screen showing a UI before user seeks access to the device 6. As indicated, the device is locked and requires the walk-up user to log in.

[0038] Figure 6 is a screen shot of the display screen

BNSDOCID: <EP_____1320008A2_I_>

showing a UI through which user would log in to the device 6. In the example of Figure 6, the user logs in by providing a username and password, which are transmitted in a secure manner to server 8.

[0039] Figure 7 is a screen shot of the display screen showing a customized service menu corresponding to services/features available to a walk-up user. Buttons 800 at the top of the screen are preferably virtual (i.e., non-physical) buttons. In this case, they represent the services of device 6 that are available to the user (i.e., scanftp, logout, scopy). The portion below buttons 800 is area 701, which is a display of a job corresponding to the "scopy" service. The scopy service allows the user to scan and copy using device 6. The virtual buttons 702 on the right hand side of the screen correspond to available features (copy, number of pages, paper selection). That is, the user can copy, set the number of pages and select paper using buttons 702. Scroll buttons 703 allow the user to scroll through the job listings displayed in area 701.

[0040] Figure 8 is a screen shot of the display screen showing another example of a customized service menu corresponding to services/features available to a walk-up user. In the example of Figure 8, area 701 corresponds to an "Hold&Print" service of the device 6 and provides a list of "Hold&Print" jobs. The screen includes buttons 800, which, in this case, correspond to the "Hold & Print", "Scan FTP", and "Logout" services of device 6. The "Hold&Print" service allows the user to store-up print jobs and to initiate printing of a stored job at device 6. The virtual buttons 802 on the right hand side of the screen correspond to available features (update list, print job and delete job). That is, the user can update/refresh list, print a job, or delete a job using buttons 802. Scroll buttons 703 allow the user to scroll through the job listing displayed in area 701.

[0041] Figure 9 is a screen shot of the display screen showing a UI though which walk-up user would log out of the device 6. Similar to Figure 8, the screen includes buttons 800, which, in this case, correspond to the "Scan FTP", "scopy", and "Logout" services of device 6.

[0042] In a case that the UI includes "unauthorized" selections, these selections may be disables such that the keys corresponding to unauthorized services/features are grayed out. The user then proceeds to use the device 6 in accordance with the determined level of access by activating non-grayed out keys that are displayed on the I/O unit 76 preferably through a touch screen.

[0043] Figure 10 illustrates a flow diagram of process steps of a networked peripheral device to manage and/or control access to the device by a walk-up user according to the present invention. In step S1001 the device 6 inquires into whether user has provided authentication information to the device 6 (e.g., authentication information received via the screen depicted in Figure 6.) A job is not initiated by the device until such information is provided by the user.

[0044] Step S1002 causes the authentication information entered by user in step S1001 to be forwarded to authenticator 48. The authenticator 48, compares or tests the authentication information provided by the user against access policy information that is stored in the directory service 47, and transmits the results back to the device 6. At step S103, device 6 awaits the results from the server 8. Step S1004 inquires into the user's success in being authenticated by the authenticator 48 based on the results received from server 8.

[0045] Should the user be unsuccessful in obtaining authentication, step S1005 causes an "access denied" message to be displayed by the device 6, thus denying the user access to any service/features of the device 6. In case of successful authentication by the user for the job requested, the device 6 determines the user's level of access to the services/features of the device 6 based on the received access policy information per step S1006. Step S1007 causes the device 6 to create a customized menu for the user based on the determined level of access.

[0046] A remote user may access device 6, for example, via a workstation such a computing equipment 1. However, the process in which a remote user accesses device 6, differs from that of a walk-up user. The following example concerns a remote user who seeks to print a job using device 6 from a workstation and an application that exists on the workstation.

1. The user initiates a print operation from within the application.

2. Device 6 determines the server 8 on which the authenticator 48 is running on.

3. A secure pipe is created between the print driver and the authenticator 48, in which the authentication information is sent to server 8.

4. The device driver 54 on the workstation transmits a request to server 8 for access policy information. The request identifies the user and device 6. Driver also provides authentication in conjunction with the request.

5. Authenticator 48 performs authentication and based on the outcome of authentication transmits a response (e.g., "access denied" or access policy information) to device 6.

6. Driver forwards the received access policy information to device 6 along with the job submitted by the user.

[0047] Figure 11 illustrates a flow diagram of process steps to manage and/or control access to a networked peripheral device by a remote user according to an embodiment of the present invention. The user logs into the

BNSDOCID: <EP_____1320008A2_I_>

network 7 in step S1101. At step S1102 a determination is made as to whether user has initiated a job request. Once the job request is initiated, device driver 54 requests access policy information that corresponds with the user and for device from sever 8 and provides authentication information to the server 8, per step S1103. Authentication information is preferably provided via a challenge and response mechanism, but can also be provided through other means such as user's username and password.

[0048] In step S1104, the server 8 sends access policy information back to the driver. Step S1105 causes the driver to forward the access policy information along with the job request to the device 6. In step S1106, the device 6 determines the user's level of access based on the received access policy information. In step S1107, the device 6 compares or tests the requested services/features against the user's level of access to determine whether the user's request conforms to the user's level of access.

[0049] A determination that the user's job request does not conform to the user's determined level of access. results in an "access denied" condition, per step S1108, thus denying the user's job request. Preferably, a message is sent to the user's workstation to alert the user of the "access denied" condition. Should the inquiry in step S1107 result in the determination that the user's job request does conform to the user's determined level of access, then step S1109 causes the device 6 to perform the requested job in accordance with the determined level of access.

[0050] Figure 11 provides a general overview of steps performed to control/manage access to device 6. Figure 12 illustrates the perspective of device 6. That is, Figure 12 illustrates a flow diagram of process steps for a networked peripheral device to manage and/or control access to the device by a remote user according to the present invention. In order to process a job that is remotely sent to a device 6, the device 6 needs to have both the requested services/features and the access policy information for the user. The job that is submitted by the user identifies the requested services/features. Device driver 54 provides the access policy information, which it received from server 8 as part of the job stream sent to device 6.

[0051] In step S1201, device driver 54 forwards the user's job to the device 6. The device 6, per step S1202, asks whether the user's access policy information is included along with the job request. If user's access policy information is not included along with the job request, then step S1203 causes an error message to be sent back to the driver 54, denying the user access to the requested services/features.

[0052] If the user's access policy information is included along with the job request, then step S1204 proceeds to determine the user's level of access based on the received access policy information. In step S1205, the device 6 compares or tests the requested services/features against the user's level of access to determine whether the user's request conforms to the user's level of access. A determination that the user's job request does not conform to the user's determined level of access, results in an error message, per step S1206, that is sent to driver 54, thus denying the user's job request. Should the inquiry in step S1205 result in the determination that the user's job request does conform to the user's determined level of access, then step S1207 causes the device 6 to perform the requested job.

[0053] Server 8 is configured to provide access policy information for a walk-up user and preferably for all enterprise users (i.e., walk-up and remote users) once the user has been authenticated by server 8.

[0054] Figure 13 illustrates a flow diagram of process steps of a server to manage and/or control access to the device by a remote user or walk-up user according to the present invention. In step S1301, server 8 awaits an access policy request and authentication information from the device 6 or driver 54. In step S1302 the authenticator 48, located on the server 8, retrieves authentication information from directory service 47. In step S1303, the retrieved information is compared or tested against the user authentication information received per step S1301. Step S1304 inquires into whether user has been successfully authenticated. If the user is unsuccessful in obtaining authentication then step S1305 causes an "access denied" message to be sent from the server 8. If the user is successfully authenticated, access, then step S1306 causes user's access policy information to be sent from the server 8.

[0055] Server 8 may reside locally with respect to device 6, computing equipment 1, or both. In a case that the network 7 is the Internet, for example, server 8 may be remotely located with respect to device 6, computing equipment 1, or both. Even where server 8 is local, it may be preferable to use a trusted architecture in which access policy information, that is received from server 8 can be trusted.

[0056] While the invention is described above with respect to what is currently considered its preferred embodiment, it is to be understood that the invention is not limited to that described above. To the contrary, the invention is intended to cover various modifications and equivalent arrangements within the scope of the appended claims.

Claims

1. A method for controlling access to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user based on centralized access management information, the method comprising:

   receiving access management information for

BNSDOCID: <EP_____1320008A2_I_>

the walk-up user at the networked peripheral device from a centralized location;
determining, at the networked peripheral device, a level of access to the networked peripheral device that are available to the walk-up user based on the received access management information; and
allowing the walk-up user to access the to the networked peripheral device based on the determined level of access.

2. A method according to claim1, wherein the networked peripheral device is a multifunction peripheral device.

3. A method according to claim1, wherein the access management information is supplied by an authentication server once the authentication server authenticates the walk-up user based on authentication information received from the networked peripheral device.

4. A method according to claim1, wherein a user interface is devised by the networked peripheral device that is specific to the determined access level.

5. A method according to claim1, wherein buttons on a keypad on the device are enabled and/or disabled according to the determined access level.

6. A method according to claim 1, wherein the access management information is supplied by an authentication server that authenticates both the walk-up user and the remote user.

7. A method according to claim 3, wherein the authentication information is a username and/or password.

8. A method according to claim 3, wherein the authentication information is entered by inserting a smart card at the networked peripheral device.

9. A method according to claim 6, wherein the access management information is encrypted.

10. A method according to claim 3, wherein the authentication information received from the networked peripheral device is encrypted.

11. A computer-readable memory medium in which computer-executable process steps are stored, the process steps for controlling access to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user based on centralized access management information, wherein the process steps comprise:

a receiving step to receive access management information for the walk-up user at the networked peripheral device from a centralized location;
a determining step to determine, at the networked peripheral device, a level of access to the networked peripheral device that are available to the walk-up user based on the received access management information; and
an allowing step to allow the walk-up user to access the to the networked peripheral device based on the determined level of access.

12. A computer-executable program code stored on a computer readable medium, said computer-executable program code for controlling access to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user based on centralized access management information, said computer-executable program code comprising:

code to receive access management information for the walk-up user at the networked peripheral device from a centralized location;
code to determine, at the networked peripheral device, a level of access to the networked peripheral device that are available to the walk-up user based on the received access management information; and
code to allow the walk-up user to access the to the networked peripheral device based on the determined level of access.

13. An apparatus for controlling access to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user based on centralized access management information, said apparatus comprising means for performing the functions specified in any of Claims 1 to 10.

14. Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for controlling access to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user based on centralized access management information, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 10.

15. A server for use in controlling access to a networked peripheral device by a walk-up user, wherein the networked peripheral device is accessible by both the walk-up user and a remote user based on centralized access management information, the serv-

BNSDOCID: <EP_____1320008A2_I_>

er comprising:

receiving a request for access policy information, the request including authentication information;
authenticating the user using the authentication information; and
transmitting access policy information for the user, in a case that authentication of the user is successful.

16. A server according to claim 15, wherein server retrieves authentication information for the user from a directory service.

BNSDOCID: <EP_____1320008A2_I_>

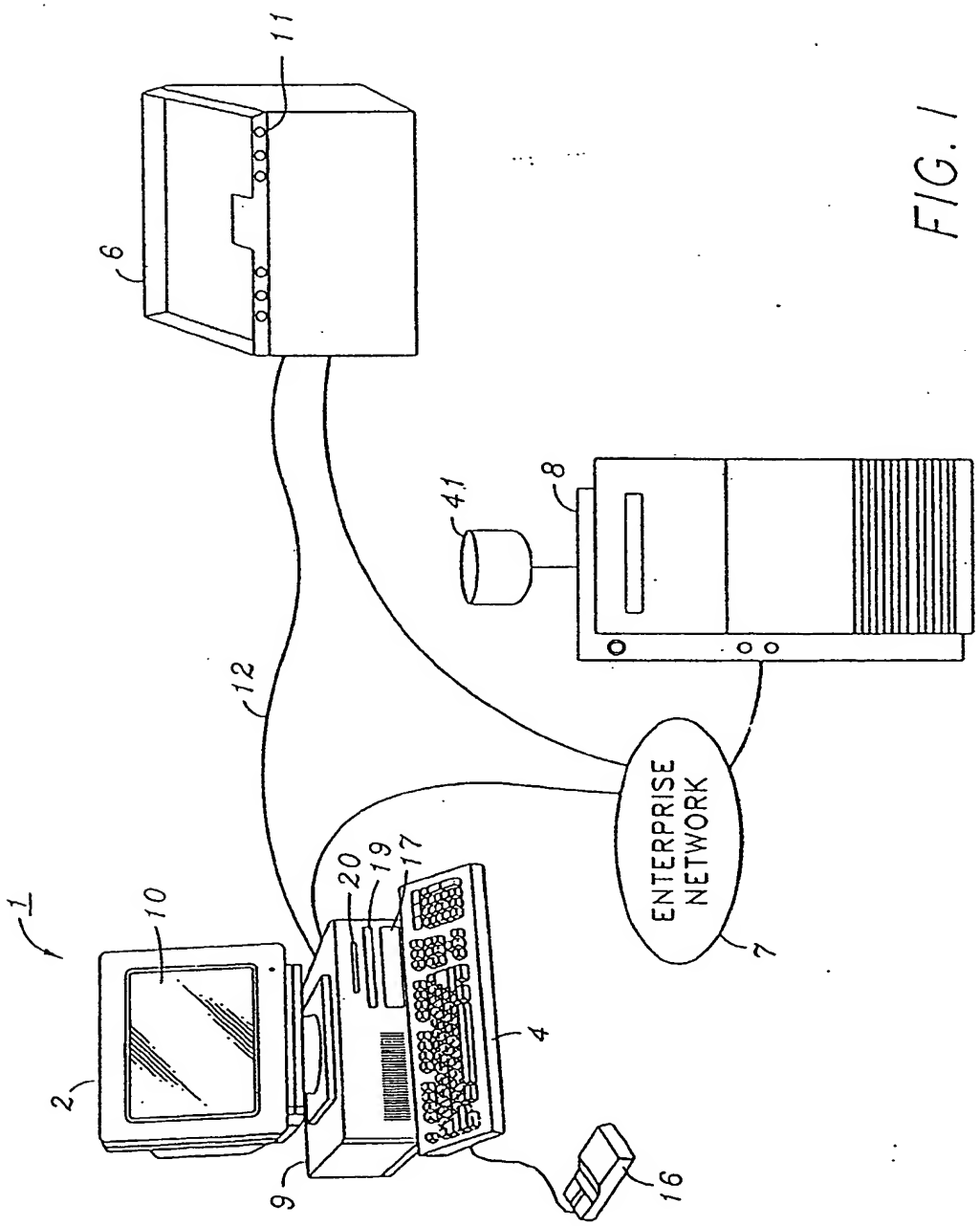

FIG. 1

BNSDOCID: <EP_____1320008A2_I_>

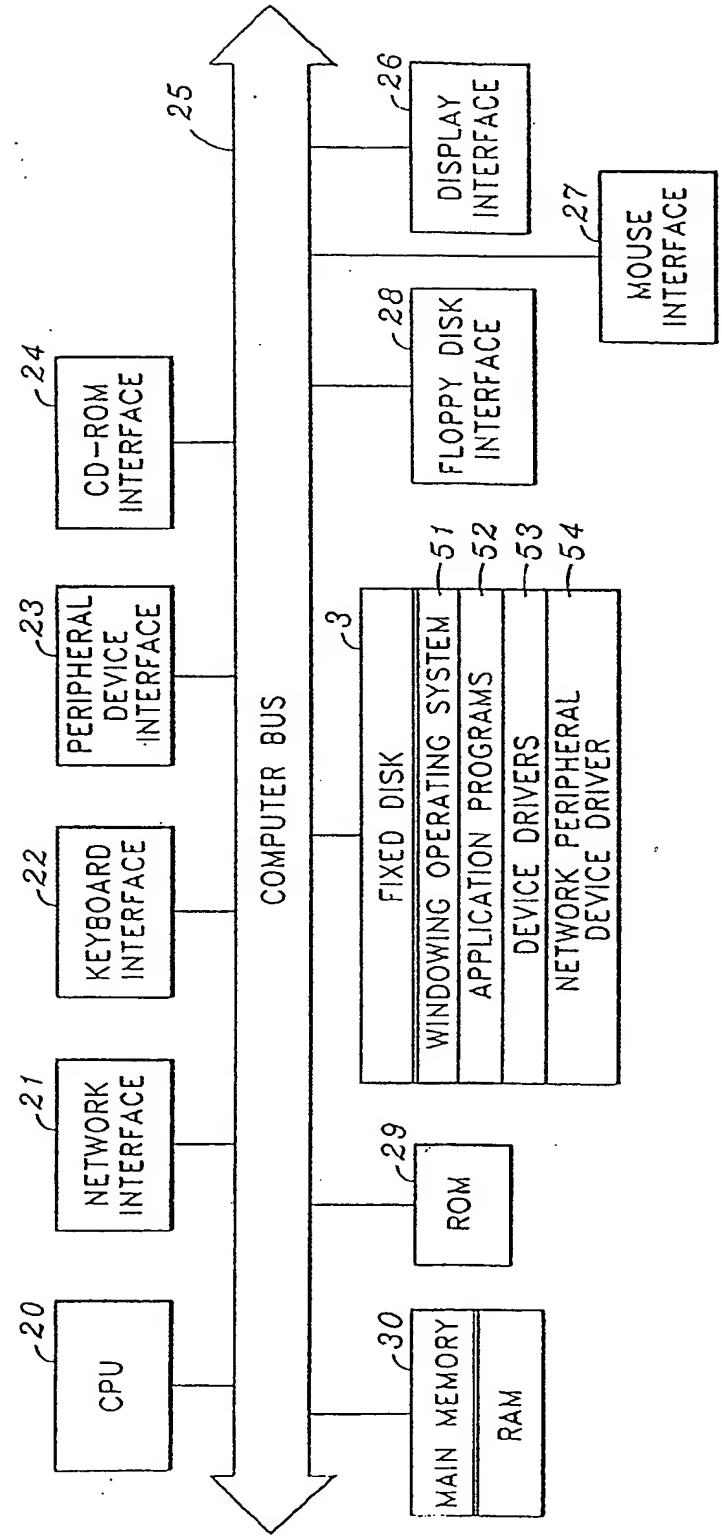

FIG. 2

BNSDOCID: <EP_____1320008A2_I_>

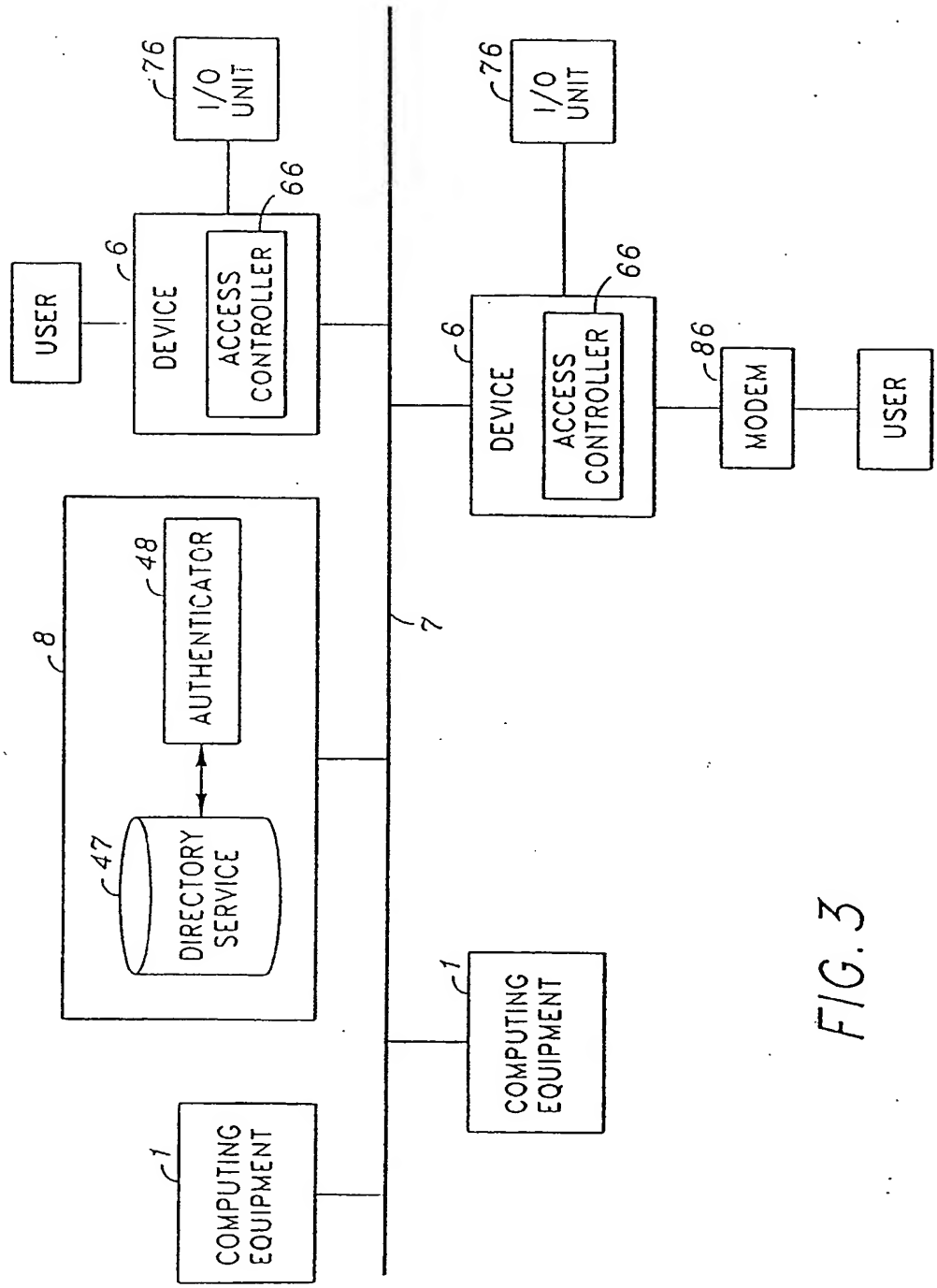

FIG. 3

BNSDOCID: <EP_____1320008A2_I_>

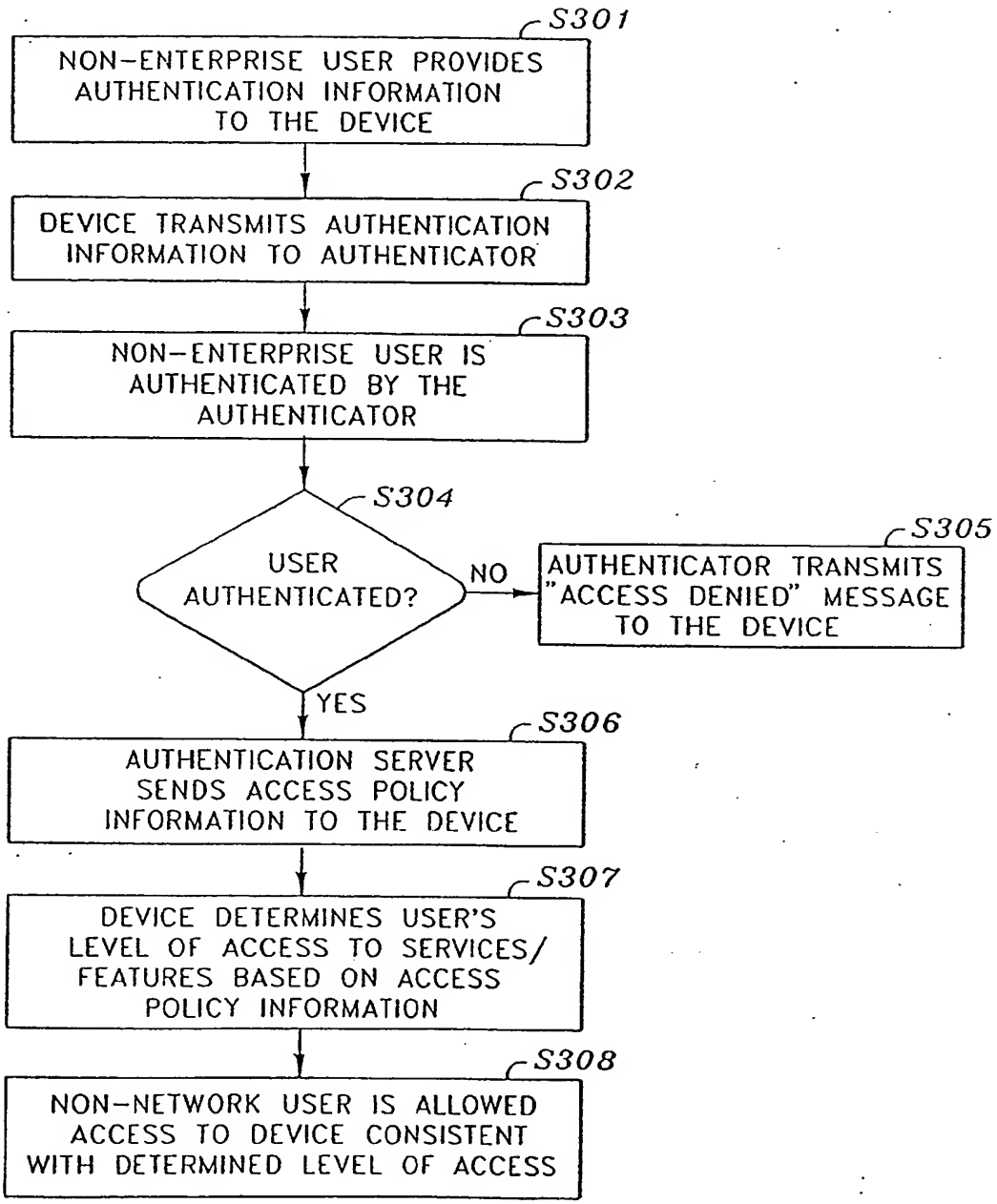

FIG. 4

BNSDOCID: <EP_____1320008A2_I_>

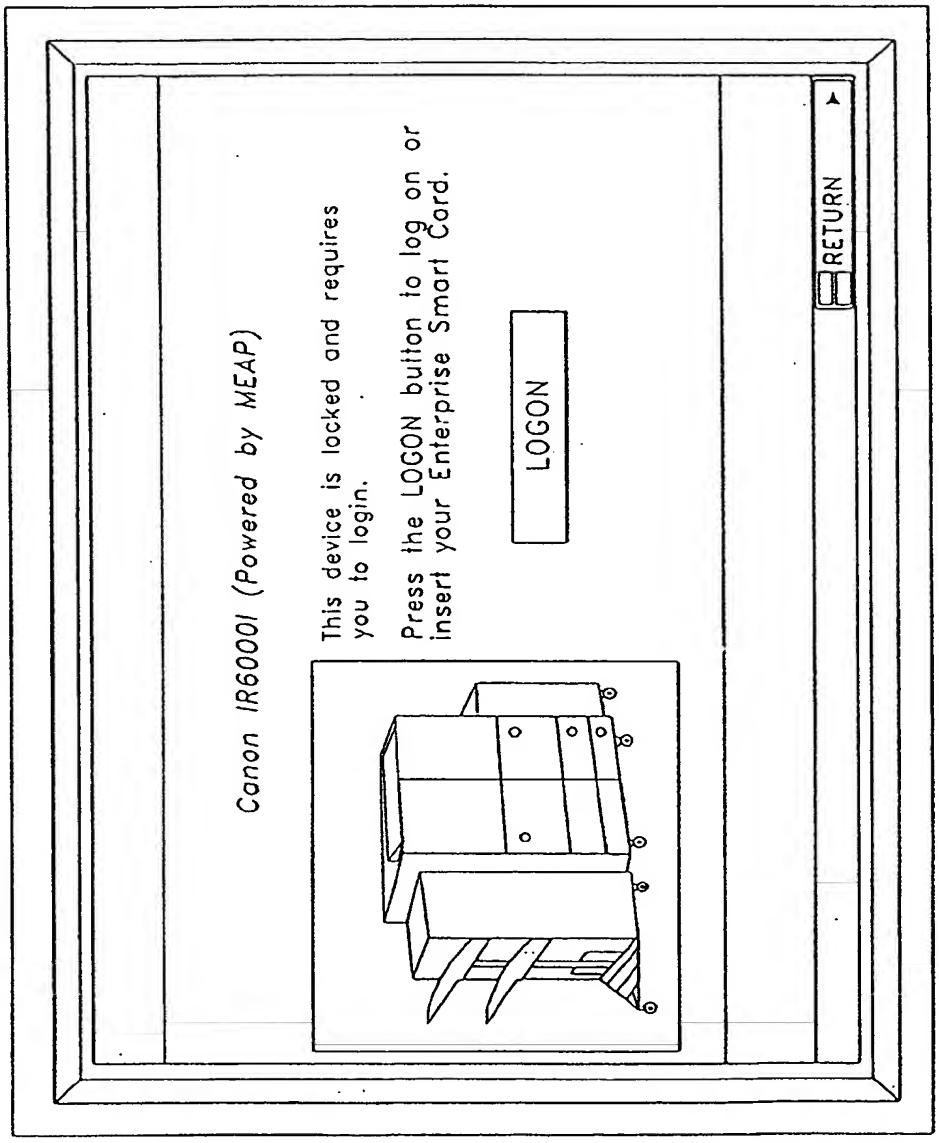

FIG. 5

BNSDOCID: <EP_____1320008A2_I_>

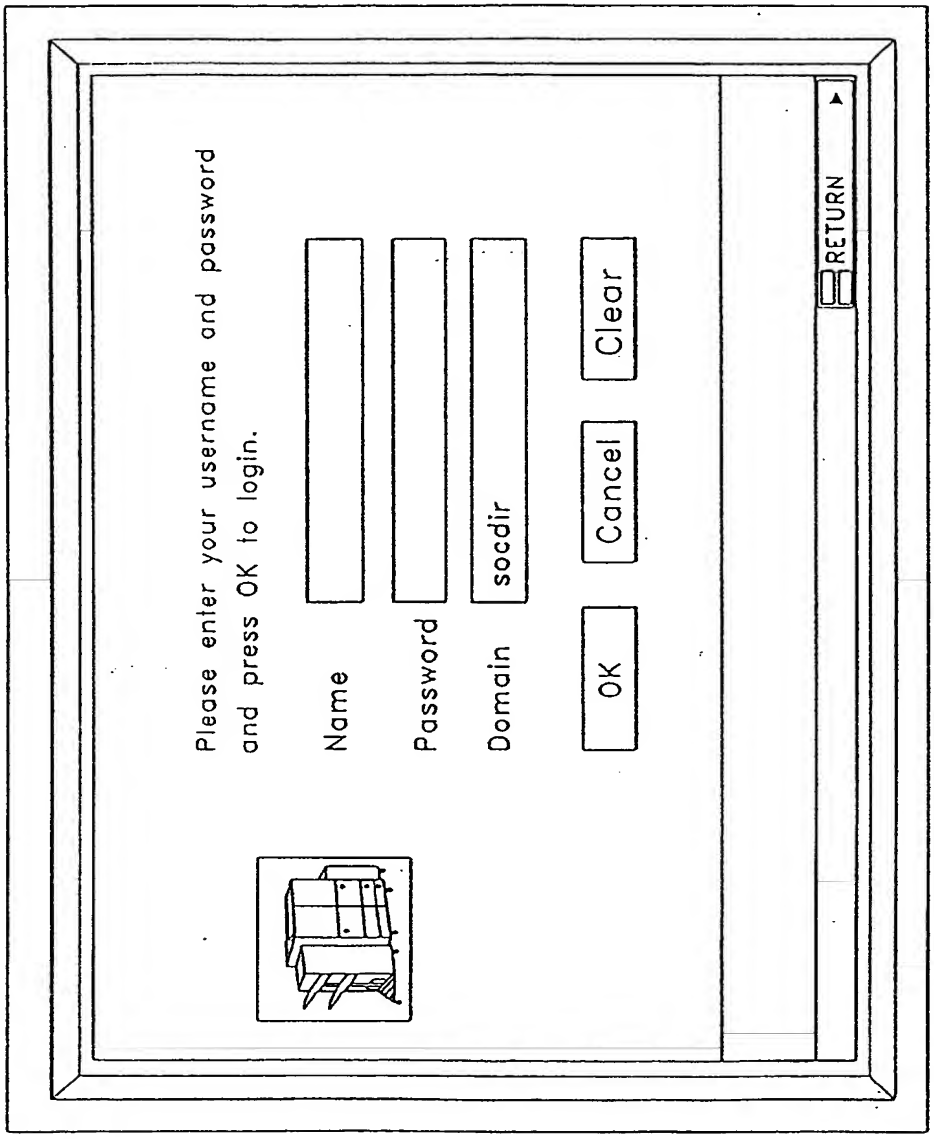

FIG. 6

BNSDOCID: <EP_____1320008A2_I_>

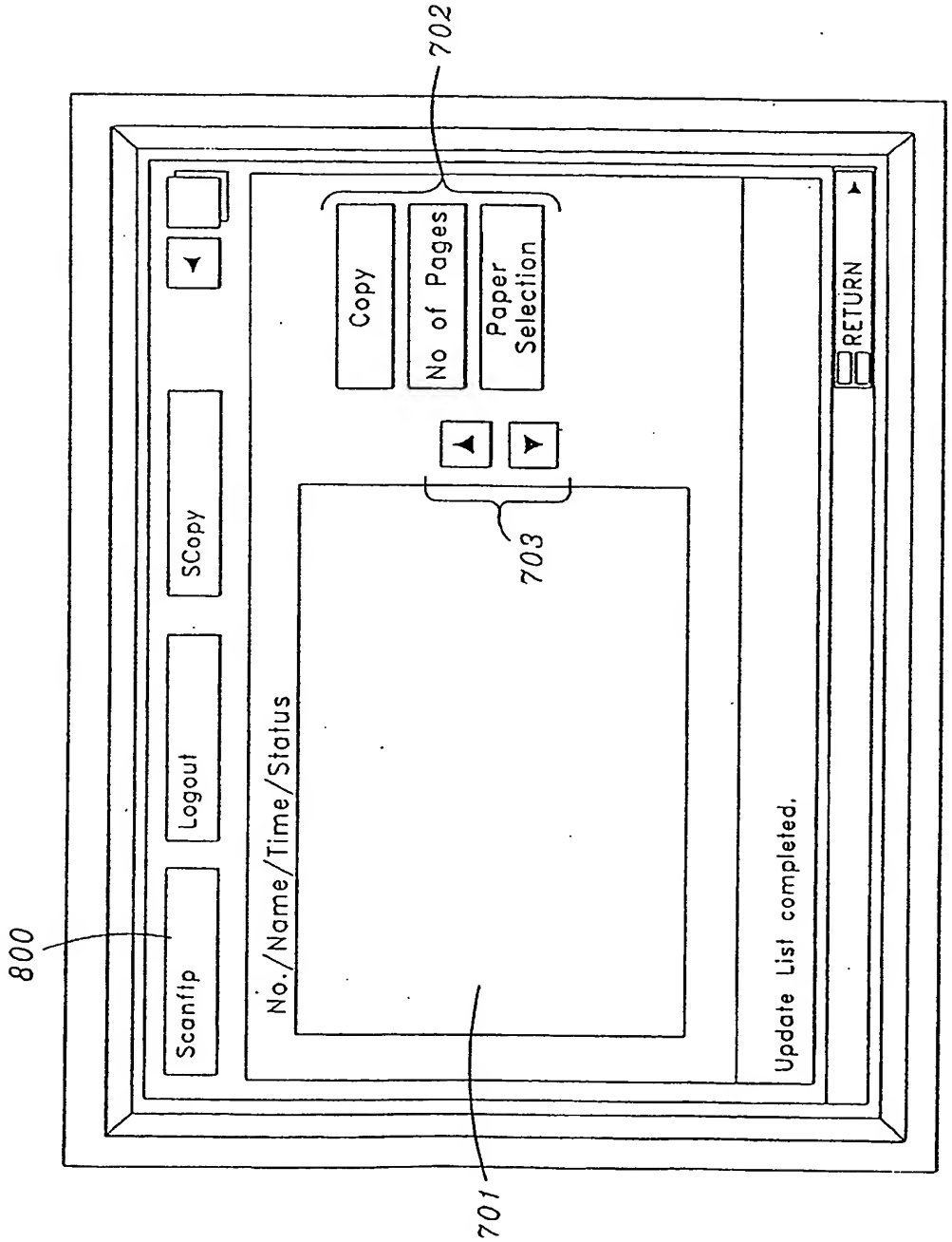

FIG. 7

BNSDOCID: <EP_____1320008A2_I_>

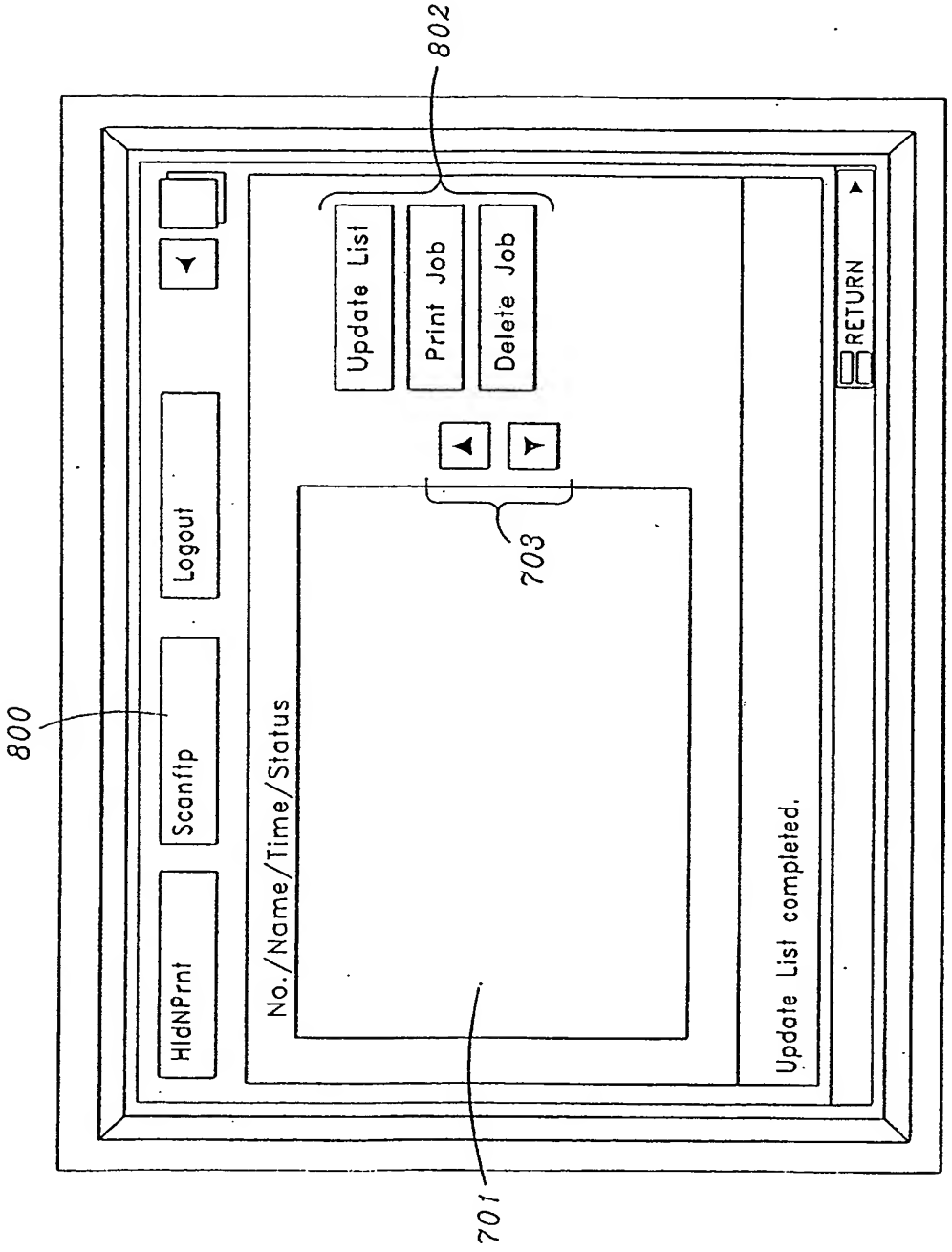

FIG. 8

BNSDOCID: <EP_____1320008A2_I_>

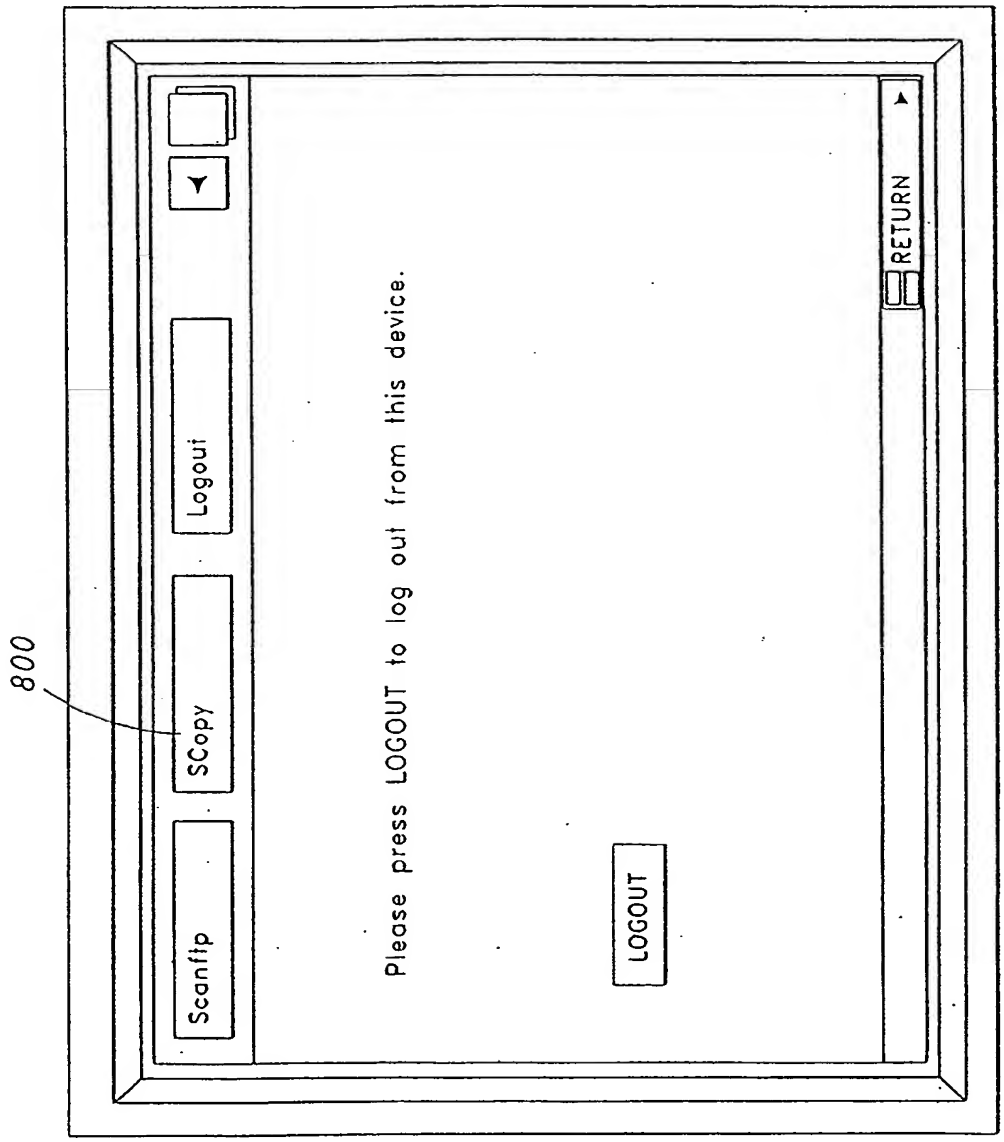

FIG. 9

BNSDOCID: <EP_____1320008A2_I_>

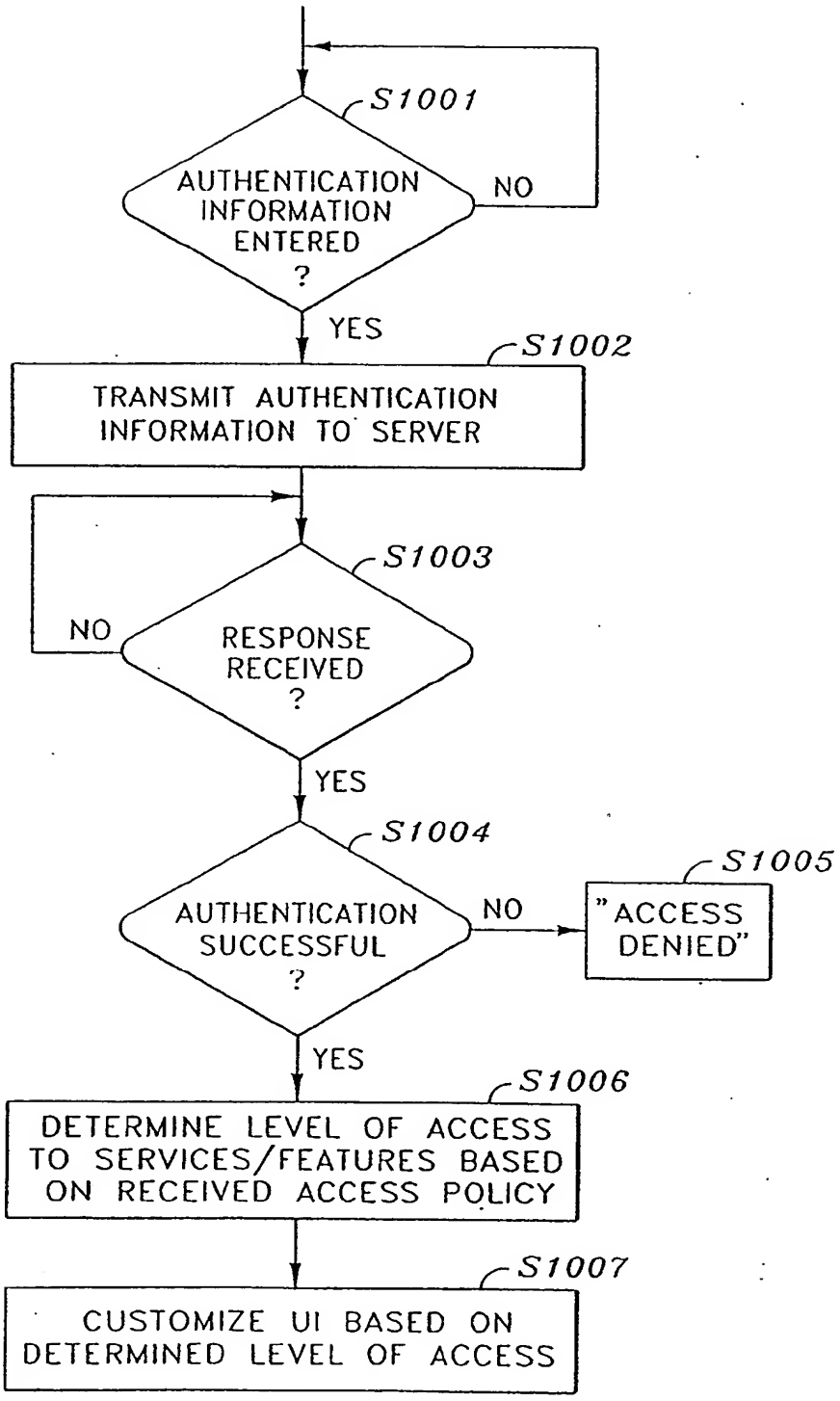

FIG. 10

BNSDOCID: <EP_____1320008A2_I_>

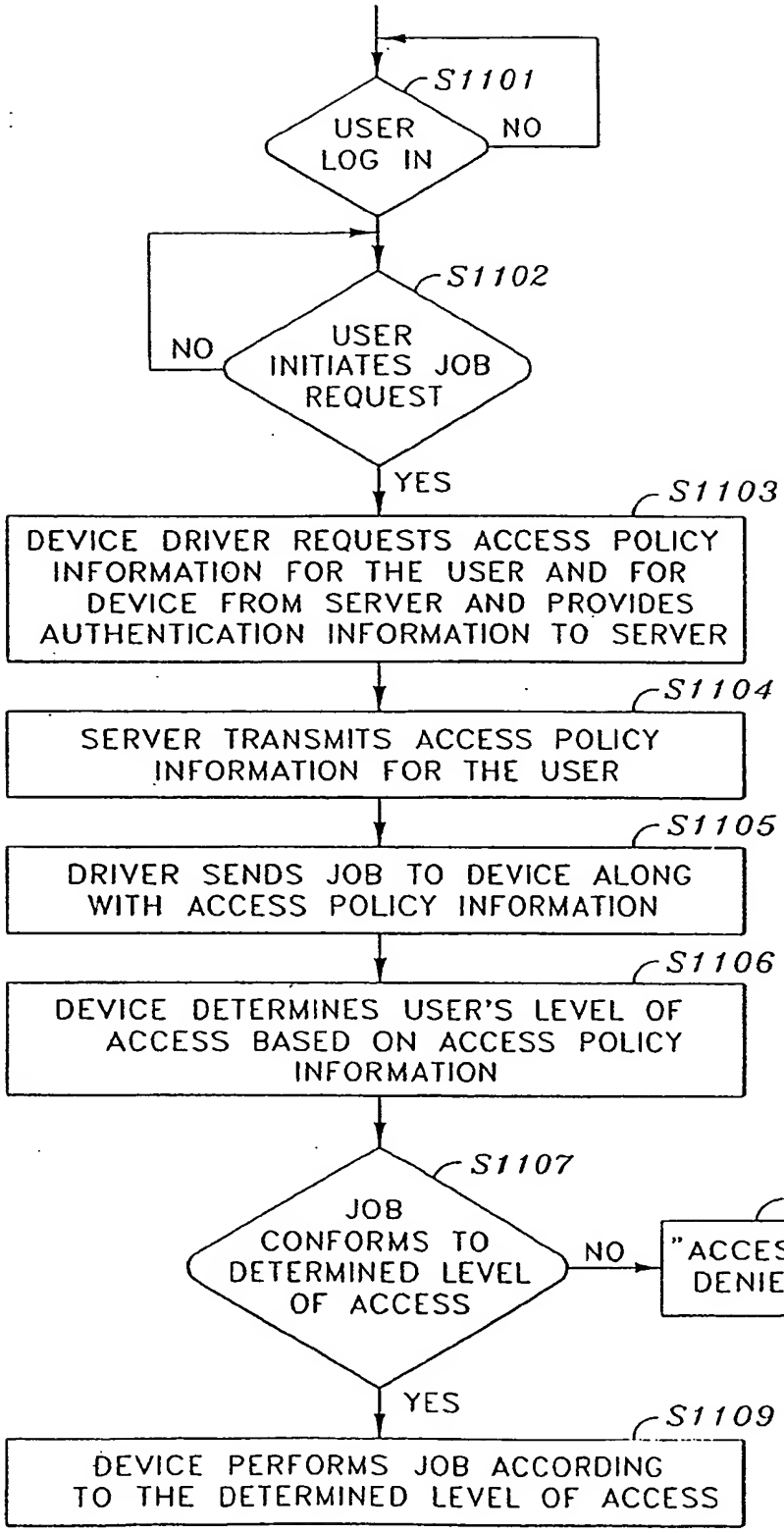

FIG. 11

BNSDOCID: <EP_____1320008A2_I_>

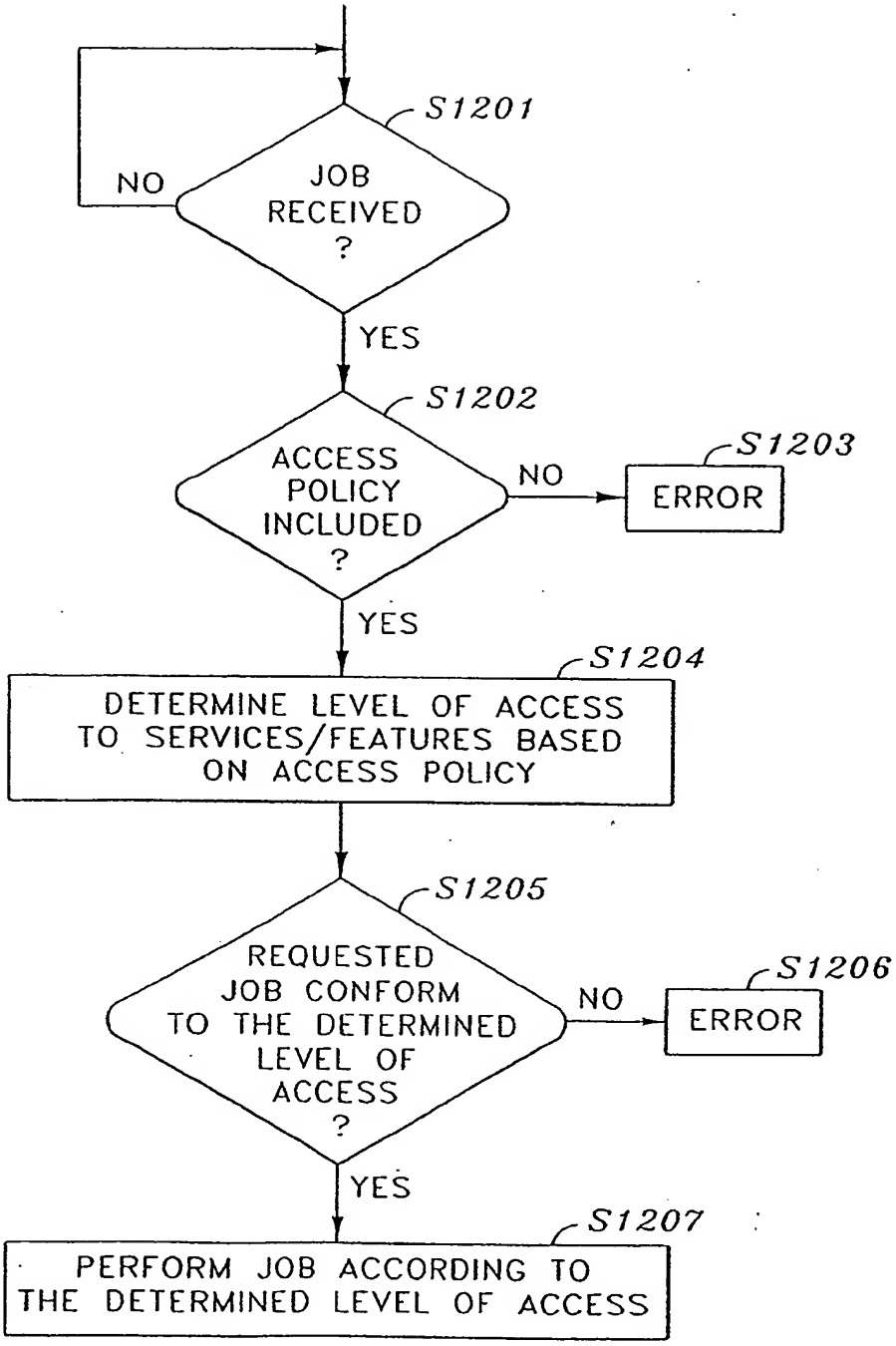

FIG. 12

BNSDOCID: <EP 1320008A2 I >

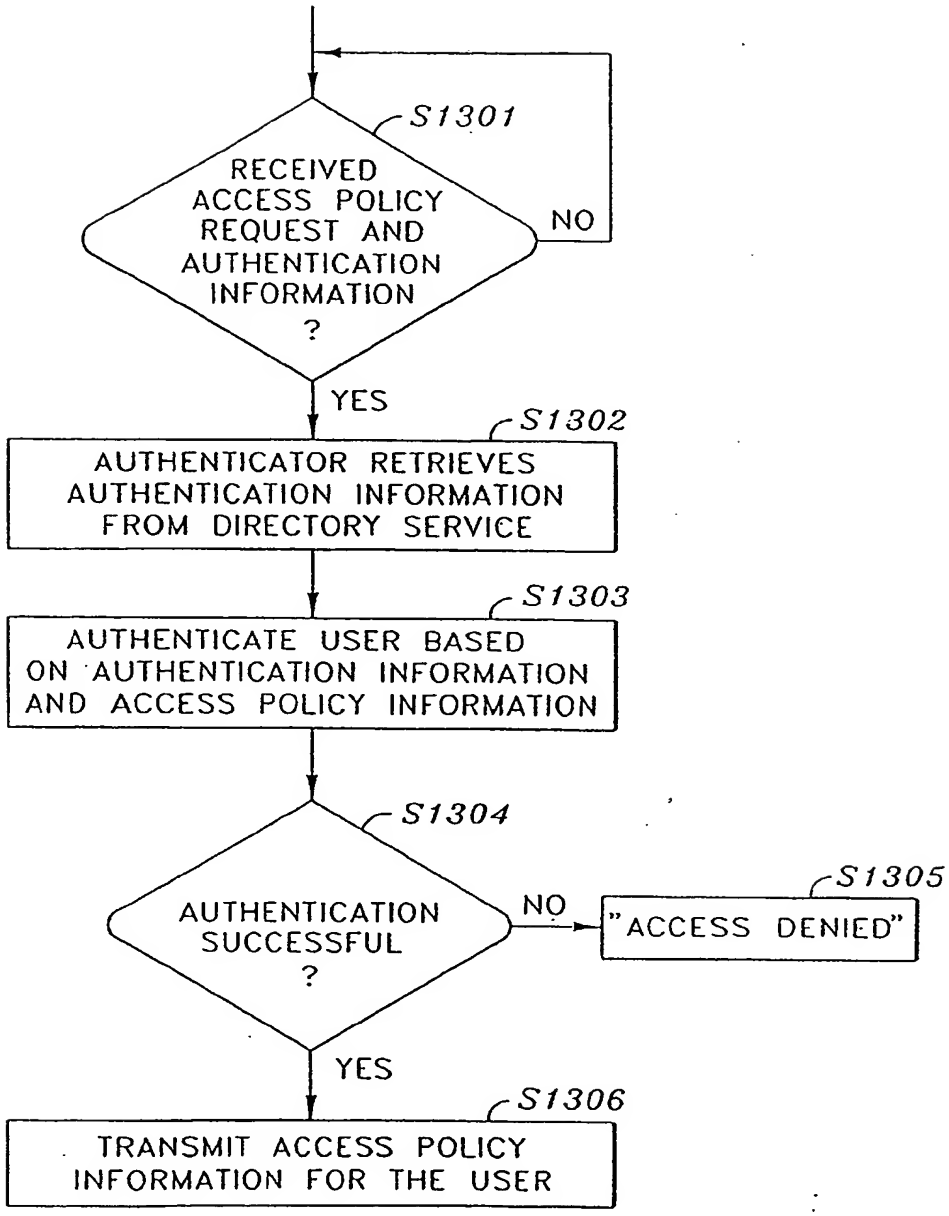

FIG. 13

BNSDOCID: <EP_____1320008A2_I_>

THIS PAGE BLANK (USP